UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,077	10/28/2003	Lane W. Lee	M-15255 US	5959

32605 7590 01/23/2007
MACPHERSON KWOK CHEN & HEID LLP
2033 GATEWAY PLACE
SUITE 400
SAN JOSE, CA 95110

EXAMINER	
KOEMPEL THOMAS, BEATRICE L	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/696,077	**Applicant(s)** LEE ET AL.	
	Examiner Bea Koempel-Thomas	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) *1-31* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-31 are pending in this application and presented for examination.

Claim Objections

2. Claim 1 is objected to for the following informalities: "the storage-engine-encrypted content key" (line 12) lacks antecedent basis. In order to further prosecution, the examiner interpreted the instance as "the first-storage-engine-encrypted content key." Appropriate correction is required.

3. Claim 31 is objected to for the following informalities: Claim 31 is apparently a dependent claim that fails to refer back to an independent claim. In order to further prosecution, the examiner considered claim 31 as depending from claim 29.

4. Appropriate correction is required.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-11 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-8 of U.S. Patent No. 7,110,982 B2 (hereinafter '982). Although the conflicting claims are not identical, they are not patentably distinct from each other because it would have been obvious to one of ordinary skill in the art at the time of the invention to construct the recited devices and to perform the recited method.

For example: Claims 1 and 2 of the instant application correspond to claim 1 of the '982 patent as follows: **Claim 1: A block-level storage device, comprising: a storage medium; and a storage engine, the storage engine being configured to generate a secure session key and to receive a block of encrypted content and its corresponding encrypted content key from a host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium. Claim 2: The block-level storage device of claim 1, wherein the storage engine is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system. (instant application).** Claim 1: A storage device comprising: a computer readable storage medium; and a computer executable storage engine, the storage engine configured to generate a secure session key and to receive encrypted content and a corresponding encrypted content key from a host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium, wherein the storage medium is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system (the ‘982 patent). Specifically, claim 1 of the ‘982 application is a broader characterization of the same invention.

Claim 3 of the instant application corresponds to claim 2 of the ‘982 patent as follows: **Claim 3: The block-level storage device of claim 2, wherein the storage engine is further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure session key only by decrypting the encrypted secure session key using the private key corresponding to the public key (instant application).** Claim 2: The storage device of claim 1, wherein the storage engine is further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure session key only by decrypting the encrypted secure session key using the private key corresponding to the public key (the ‘982 patent).

Additionally, claims 4-6 and 9-11 of the instant application correspond to claims 3-5 and 6-8 of the ‘982 patent, respectively, for the same reasons as the examples presented above.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. **Claims 1, 14-16, and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Lee et al., U.S. Patent No. 6,636,966 B1, (hereinafter "Lee '966").**

9. Regarding **claim 1**: Lee '966 discloses a block-level storage device (abstract), comprising:

a storage medium (Figs. 1 element 10, and col. 4 line 9); and

a storage engine (Fig. 1, element 14, and col. 4 lines 12-13), the storage engine being configured to generate a secure session key and to receive a block of encrypted content and its corresponding encrypted content key from a host system (col. 9 lines 39-54), wherein the content key has been encrypted by the host system using the secure session key (col. 9 lines 39-54), the storage engine being further configured to decrypt the encrypted content key using the secure session key (col. 9 lines 39-54) and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium (Fig. 2A, element 28, and col. 6 lines 6-7).

10. Regarding **claim 14** Lee '966 discloses a system, comprising:

a host system (col. 7 lines 58-65), the host system configured to request for file system objects stored by a storage device by identifying the block addresses containing a requested file system object and requesting the storage device to return the content stored at the identified block addresses (col. 7-8 lines 6-11), the host system being further configured to identify the file system object to the storage device if the requested file system object comprises secure content (col. 7-8 lines 6-11); and

a storage device (abstract lines 1-3) having:

a storage medium (Figs. 1 element 10, and col. 4 line 9), configured to store security metadata for the secure file system objects (col. 8 lines 15-29); and

a storage engine (Fig. 1, element 14, and col. 4 lines 12-13), the storage engine being configured to respond to block-level requests from the host system by retrieving the content stored at the requested block addresses from the storage medium (col. 8 lines 15-29), the storage engine being further configured to access the security metadata if the block-level requests correspond to content comprising a secure file system object (col. 8 lines 15-29).

11. Regarding **claim 15**: Lee '966 discloses that the security metadata includes a locking indicator (col. 8 lines 15-29), the storage engine being configured to prevent access to the

corresponding file system object content if the locking indicator indicates the file system object is locked (col. 8 lines 15-29).

12. Regarding **claim 16**: Lee '966 discloses that the storage engine is configured to change the security metadata for a secure file system object in response to an Internet transaction with a validated host system (col. 9 lines 3-16).

13. Regarding **claim 22**: Lee '966 discloses that the storage engine (Fig. 1, element 14, and col. 4 lines 12-13), is configured to generate a secure session key (col. 9 lines 39-54), the storage engine generating the security metadata for each secure file system object by receiving a corresponding encrypted content key from the host system (col. 9 lines 39-54), wherein the content key has been encrypted by the host system using the secure session key (col. 9 lines 39-54), the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium (Fig. 2A, element 28, and col. 6 lines 6-7).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary

> skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. **Claims 2-11, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee '966 in view of Feldman et al., U.S. Patent Publication No. 2003/0115147 A1, (hereinafter "Feldman").**

16. Applicant has provided evidence in this file showing that the invention may have been subject to an obligation of assignment to the same entity as Lee '966 and Feldman at the time this invention was made. However, references Lee '966 and Feldman additionally qualify as prior art under another subsection of 35 U.S.C. 102, and therefore, are not disqualified as prior art under 35 U.S.C. 103(c).

Applicant may overcome the applied art either by a showing under 37 CFR 1.132 that the inventions disclosed therein were derived from the invention of this application, and are therefore, not the invention "by another," or by antedating the applied art under 37 CFR 1.131.

17. Regarding **claim 11**: Lee '966 discloses encrypting the content key using the secure session key and transmitting the encrypted content key to the block-level storage device (col. 9 lines 39-54).

Lee '966 does not disclose a method of writing to a block-level storage device from a host system having a public key and a corresponding private key, comprising: encrypting a secure session key using the public key; recovering the secure session key from the encrypted secure session key using the corresponding private key; encrypting content according to a content key and commanding the block-level storage device to write the encrypted content to host-system-determined block addresses; or in the block-level storage device, decrypting the encrypted content key using the secure session key.

Feldman discloses a method of writing to a block-level storage device from a host system having a public key and a corresponding private key, comprising:

encrypting a secure session key using the public key (page 11, [0168], lines 6-14);

recovering the secure session key from the encrypted secure session key using the corresponding private key (page 11, [0168], lines 6-14);

encrypting content according to a content key (page 7, [0123]) and commanding the block-level storage device to write the encrypted content to host-system-determined block addresses (page 15, [0199] and page 19, [0249]), the content key comes from a server and can include file directory information); and

in the block-level storage device, decrypting the encrypted content key using the secure session key (page 7, [0123]).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the security methods taught by Feldman in order to create a seamless security system for electronic content (*See* Feldman page 4, [0077], lines 9-10).

18. Regarding **claim 2**: Lee '966 does not disclose that the storage engine is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system.

Feldman discloses that the storage engine is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system (Fig. 6 and page 11, [0168]).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the security methods taught by Feldman in order to create a seamless security system for electronic content (*See* Feldman page 4, [0077], lines 9-10).

19. Regarding **claim 3**: Lee '966 does not disclose that the storage engine is further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure session key only by decrypting the encrypted secure session key using the private key corresponding to the public key.

Feldman discloses that the storage engine is further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure session key only by decrypting the encrypted secure session key using the private key corresponding to the public key (page 11, [0168], lines 6-14).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the security methods taught by Feldman in order to create a seamless security system for electronic content (*See* Feldman page 4, [0077], lines 9-10).

20. Regarding **claim 4**: Lee '966 discloses that the storage engine is further configured to re-encrypt the block of encrypted content using at least a second storage engine encryption key (col. 11 lines 37-54).

21. Regarding **claim 5**: Lee '966 discloses that the second storage engine encryption key comprises a Data Encryption Standard (DES) key (col. 11 lines 22-37).

22. Regarding **claim 6**: Lee '966 discloses that the DES key comprises a triple DES key (col. 11 lines 22-37).

23. Regarding **claim 7**: Lee '966 discloses that the storage engine is a hard disc storage engine and wherein the storage media is a hard disc (col. 15 lines 18-34).

24. Regarding **claim 8**: Lee '966 discloses that the storage media is a removable hard disc (col. 15 lines 18-34).

25. Regarding **claim 9**: Lee '966 discloses that the public key and the private key are elliptic curve cryptography keys (Table 3, ECC public key and ECC private key).

26. Regarding **claim 10**: Lee '966 discloses that the storage engine includes a random number generator for generating the secure session key (Table 1, engine generates random key).

27. Regarding **claim 31**: Lee '966 discloses a block-level storage device including a storage engine (Fig. 1, element 14, and col. 4 lines 12-13).

Lee '966 does not disclose that the storage engine is configured to receive a public key from the host system and to encrypt the secure session key with the public key and to send the encrypted secure session key to the host system, whereby the host system may recover the secure session key only through the use of the host system's corresponding private key.

Feldman discloses that the storage engine is configured to receive a public key from the host system and to encrypt the secure session key with the public key and to send the encrypted secure session key to the host system, whereby the host system may recover the secure session key only through the use of the host system's corresponding private key (page 11, [0168], lines 6-14).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the security methods taught by Feldman in order to create a seamless security system for electronic content (*See* Feldman page 4, [0077], lines 9-10).

28. **Claims 23-26, 29, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee '966 in view of Lee et al., U.S. Patent No. 6,823,398 B1, (hereinafter "Lee '398").**

29. The applied reference, Lee '398, has a common inventor with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was

derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). This rejection might also be overcome by showing that the reference is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

30. Regarding **claim 23**: Lee '966 discloses a system, comprising: a host system, the host system being configured to request for non-secure file system objects by identifying the block addresses corresponding to the non-secure file system object and to request for secure file system objects by identifying the file system object (col. 7-8 lines 12-11).

Lee '966 does not disclose a storage device having: a storage medium configured to store security metadata for the secure file system objects; and a storage engine, wherein the storage engine is configured to control the file system used to store secure and non-secure file system objects on the storage medium, the storage engine being further configured to respond to block-level requests for non-secure file system objects by translating the block-level requests from the host system to byte-level offsets within a file system object on the storage medium, the storage engine being further configured to control the file system associated with secure file system objects by determining where secure file system objects will be stored on the storage medium and where the corresponding security metadata will be stored on the storage medium.

Lee '398 discloses a storage device having:

a storage medium configured to store security metadata for the secure file system objects (col. 6 lines 15-24); and

a storage engine, wherein the storage engine is configured to control the file system used to store secure and non-secure file system objects on the storage medium, the storage engine being further configured to respond to block-level requests for non-secure file system objects by translating the block-level requests from the host system to byte-level offsets within a file system object on the storage medium, the storage engine being further configured to control the file system associated with secure file system objects by determining where secure file system objects will be stored on the storage medium (col. 5-6 lines 50-14) and where the corresponding security metadata will be stored on the storage medium (col. 7 lines 6-32).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the storage device incorporating file system management as taught by Lee '398 in order to protect against unauthorized copying and distribution of media, (*See* Lee '398 col. 1 lines 15-25).

31. Regarding **claim 29**: Lee '966 discloses a block-level storage device (abstract), comprising:

a storage medium (Figs. 1 and 10, and col. 4 line 9).

Lee '966 does not disclose a storage engine, the storage engine being configured to respond to block-level non-secure content requests, block-level secure content requests, and block-level security metadata requests from a host system, the storage engine being further configured to, in response to a security metadata request, generate a secure session key and to receive an encrypted content key from the host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium.

Lee '398 discloses a storage engine, the storage engine being configured to respond to block-level non-secure content requests, block-level secure content requests, and block-level security metadata requests from a host system, the storage engine being further configured to, in response to a security metadata request, generate a secure session key and to receive an encrypted content key from the host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key (col. 5-6 lines 50-14) and to write the storage-engine-encrypted content key to the storage medium (col. 7 lines 6-32).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the storage device incorporating file system management as taught by Lee

‘398 in order to protect against unauthorized copying and distribution of media, (*See* Lee ‘398 col. 1 lines 15-25).

32. Regarding **claim 24**: Lee ‘966 discloses that the storage engine is a hard disc storage engine and wherein the storage media is a hard disc (col. 15 lines 18-34).

33. Regarding **claim 25**: Lee ‘966 discloses that the storage media is a removable hard disc (col. 15 lines 18-34).

34. Regarding **claim 26**: Lee ‘966 discloses that the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system object content if the locking indicator indicates the file system object is locked (col. 8 lines 15-29).

35. Regarding **claim 30**: Lee ‘966 discloses that the storage engine includes a random number generator for generating the secure session key (Table 1, engine generates random key).

36. **Claims 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee ‘966 in view of Ta et al., U.S. Patent No. 7,168,787 B1, (hereinafter “Ta”).**

37. Regarding **claim 17**: Lee ‘966 does not disclose that the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played

by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights.

Ta discloses that the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights (col. 12-13 lines 46-53 and col. 14 lines 17-24).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the play control taught by Ta in order to create media that would be self-protecting against unauthorized viewing, (*See* Ta col. 5 lines 20-28).

38. Regarding **claim 18**: Lee '966 does not disclose that the storage engine is configured to erase the security metadata if the play flag indicates that the host system has no remaining play rights.

Ta discloses that the storage engine is configured to erase the security metadata if the play flag indicates that the host system has no remaining play rights (col. 15-16 lines 14-9).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the play control taught by Ta in order to create media that would be self-protecting against unauthorized viewing, (*See* Ta col. 5 lines 20-28).

39. Regarding **claim 19**: Lee '966 discloses that the security metadata includes a locking indicator, the storage engine being configured to prevent access to the corresponding file system

object content if the locking indicator indicates the file system object is locked (col. 8 lines 15-29).

Lee '966 does not disclose that the storage engine is configured to assert the locking indicator if the play flag indicates that the host system has no remaining play rights.

Ta discloses that the storage engine is configured to assert the locking indicator if the play flag indicates that the host system has no remaining play rights (col. 12-13 lines 46-53 and col. 14 lines 17-24).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the play control taught by Ta in order to create media that would be self-protecting against unauthorized viewing, (*See* Ta col. 5 lines 20-28).

40. Regarding **claim 20**: Lee '966 does not disclose that the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights.

Ta discloses that the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights (col. 12-13 lines 46-53 and col. 14 lines 17-24).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the copy control taught by Ta in order to create media that would be self-protecting against unauthorized viewing, (*See* Ta col. 5 lines 20-28).

41. Regarding **claim 21**: Lee '966 discloses that the storage engine is configured to modify security metadata for a secure file system object through an Internet transaction with an authorized host system (col. 9 lines 3-16).

42. **Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee '966 in view of Feldman, and further in view of Ansell et al., U.S. Patent No. 6,367,019 B1, (hereinafter "Ansell").**

43. Regarding **claim 12**: Lee '966 does not disclose in the block-level storage device, encrypting the decrypted content key with a storage device key; and writing the storage-device-encrypted content key to a host-system-determined block address.

Feldman discloses writing the storage-device-encrypted content key to a host-system-determined block address (page 15, [0199] and page 19, [0249]).

Feldman does not disclose in the block-level storage device, encrypting the decrypted content key with a storage device key.

Ansell discloses in the block-level storage device, encrypting the decrypted content key with a storage device key (col. 7 lines 14-37).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Lee '966 and Feldman with the storage device key as taught by Ansell in order to bind access authorization to a specific storage device, (*See* Ansell col. 2 lines 5-13).

44. Regarding **claim 13**: Lee '966 discloses that the content comprises a file system object (col. 15 lines 18-34).

Lee '966 does not disclose the method further comprising: in the block-level storage device, encrypting the decrypted content key with a storage device key, and writing the storage-device-encrypted content key to a storage-device-determined block address.

Feldman discloses writing the storage-device-encrypted content key to a storage-device-determined block address (page 15, [0199] and page 19, [0249]).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Lee '966 by the security methods taught by Feldman in order to create a seamless security system for electronic content (*See* Feldman page 4, [0077], lines 9-10).

Feldman does not disclose in the block-level storage device, encrypting the decrypted content key with a storage device key.

Ansell discloses in the block-level storage device, encrypting the decrypted content key with a storage device key (col. 7 lines 14-37).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Lee '966 and Feldman with the storage device key as taught by

Ansell in order to bind access authorization to a specific storage device, (*See* Ansell col. 2 lines 5-13).

45. **Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee '966 in view of Lee '398, and further in view of Ta.**

46. Regarding **claim 27**: Lee '966 and Lee '398 do not disclose that the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights.

Ta discloses that the security metadata includes a play flag, the play flag indicating how many times the corresponding file system object may be played by the host system, the storage engine being configured to prevent access to the corresponding file system object if the play flag indicates that the host system has no remaining play rights (col. 12-13 lines 46-53 and col. 14 lines 17-24).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Lee '966 and Lee '398 with the play control taught by Ta in order to create media that would be self-protecting against unauthorized viewing, (*See* Ta col. 5 lines 20-28).

47. Regarding **claim 28**: Lee '966 and Lee '398 do not disclose that the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights.

Ta discloses that the security metadata includes a copy flag, the copy flag indicating how many times the host system may copy the corresponding file system object, the storage engine being configured to prevent access to the corresponding file system object if the copy flag indicates that the host system has no remaining copy rights (col. 12-13 lines 46-53 and col. 14 lines 17-24).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the combination of Lee '966 and Lee '398 with the copy control taught by Ta in order to create media that would be self-protecting against unauthorized viewing, (*See* Ta col. 5 lines 20-28).

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- Chien, U.S. Patent Publication No. 2003/0233462 A1, regarding a system and method for providing a digital rights scheme for browser downloads.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Thursday & alternate Fridays; 0730 - 1700.

If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Gilberto Barron, at 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

bkt 1/17/2007

N. ElHady
NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER